UNDER SEAL

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA, v. KWASHIE SENAM ZILEVU, Defendant.	**UNDER SEAL** Case No. 1:19-mj-430

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT AND ARREST WARRANT

Your affiant, Flannan Soden, being duly sworn, hereby deposes and states as follows:

INTRODUCTION

1. I am a Special Agent with the Treasury Inspector General for Tax Administration ("TIGTA") and have been since November 2016. I am currently assigned to the Mid-Atlantic Field Division – New Carrollton, Maryland Office. I am a graduate of the Criminal Investigator Training Program at the Federal Law Enforcement Training Center as well as the TIGTA Special Agent Basic Training Academy. Prior to becoming a Special Agent, I was an Investigative Specialist for a year and four months with TIGTA. Prior to my career with TIGTA, I was a Taxpayer Advocate with the Internal Revenue Service ("IRS") for approximately 6 years.

2. As a TIGTA agent, I have received instruction and training, including the use of computers, cell phones, social media, email, and the internet in connection with criminal activity. In particular, I have experience investigating the impersonation of IRS officials, theft of IRS property, bribery, unauthorized disclosure of tax return information, loss of IRS property and equipment, and threats to and assaults on the IRS and its employees. In the course of conducting or participating in criminal investigations, I have interviewed and debriefed witnesses and

informants; conducted physical surveillance; analyzed bank records and other financial documents; analyzed telephone records; and collected and analyzed evidence.

3. I submit this affidavit in support of a criminal complaint charging KWASHIE SENAM ZILEVU ("ZILEVU") with knowingly committing Access Device Fraud, in violation of Title 18, United States Code, Section 1029(a)(5). This affidavit is also submitted in support of an arrest warrant.

4. The facts and information contained in this affidavit are based upon my personal knowledge of the investigation and information conveyed to me by other state and federal law-enforcement. All observations that I did not personally make were related to me by the individuals who made them, or come from my review of reports, documents, records, and other physical evidence obtained during the course of this investigation. This affidavit contains information necessary to establish probable cause. It does not include each and every fact known by me or known by the government.

PROBABLE CAUSE

5. TIGTA is investigating potential violations of 18 U.S.C. § 1029(a)(5) (Access Device Fraud) and other related criminal offenses. During the course of the investigation, TIGTA identified three victims, Victim A, Victim B, and Victim C (collectively referred to as "the victims"), whose identities had been stolen. Further investigation revealed that from in or about January 2016 to in or about December 2017, the victims' stolen personally identifiable information ("PII") was used to obtain three credit cards. Interviews with the victims confirmed that the credit cards were obtained without their knowledge or consent.

6. The credit card applications submitted using Victim A's and Victim C's PII listed 14520 General Washington Drive, Woodbridge, Virginia 22193, as Victim A's and Victim C's

address. The card issued in Victim A's name and the card issued in Victim C's name were delivered to the listed address in Woodbridge, Virginia.

7. The email account on the credit card application submitted under Victim B's name was accessed on multiple occasions using an Internet Protocol ("IP") address linked to the 14520 General Washington Drive, Woodbridge, Virginia 22193.

8. ZILEVU owns and lives at the property located at 14520 General Washington Drive, Woodbridge, Virginia 22193 (hereinafter "ZILEVU's address").

9. Evidence obtained during the investigation shows that from in or about January 2016 to in or about February 2018, ZILEVU used the three credit cards fraudulently issued in the name of the victims to purchase approximately $69,000 in various goods and services.

10. On or about September 19, 2019, United States Postal Inspection Service ("USPIS") Postal Inspector Jackie Palmer and I interviewed ZILEVU at his place of employment ("September 2019 Interview"). During the interview, ZILEVU made the following statements:

a. He is currently employed as an Information Technology Specialist with the IRS.

b. He lives at the residence located at ZILEVU's address with his cousin, Aseye Zilevu, and another tenant to whom he rents out the basement.

c. He received the credit cards issued to the three victims.

d. He routinely used all three credit cards to purchase goods and services for his personal use.

11. The investigation has shown that ZILEVU was aware that he was using the names and identities of real persons, and not providing fictitious information. When a person submits a credit card application to a financial institution, that institution discloses the fact that pursuant to the Bank Secrecy Act and the USA Patriot Act, all financial institutions are required to obtain,

verify, and record information that identifies each person who opens an account. ZILEVU knew that if he used fictitious information, his credit card applications would not be approved. So, he knowingly and without authorization used the true names, addresses, dates of birth, and Social Security numbers of at least three real individuals to obtain fraudulent credit cards.

A. **Victim A**

12. On or about January 25, 2016, an American Express ("AMEX") application was submitted electronically using Victim A's PII. In addition to listing Victim A's true address and telephone number, the AMEX application listed Victim A's home address as ZILEVU's address, and Victim A's telephone number as Google Voice telephone number ending in 2285, which is ZILEVU's phone number (hereinafter "ZILEVU's Google number"). A review of Prince William County property records showed that ZILEVU is the current owner of the property located at ZILEVU's address and has been the owner since on or about January 16, 2014. Google's records established that the ZILEVU's Google number is assigned to ZILEVU. The AMEX credit card was issued to Victim A, and mailed to ZILEVU's address.

13. Between on or about April 30, 2016, and on or about February 24, 2017, approximately $49,000 was charged to the AMEX card. A review of the AMEX credit card statements showed that numerous transactions were made in Woodbridge, Virginia, within the Eastern District of Virginia.

14. On or about February 24, 2017, an American Express employee contacted the USPIS to report that a fraudulent credit card application with Victim A's PII had been submitted.

15. On or about April 4, September 7, and December 29, 2017, among other dates, USPIS agents conducted surveillance of ZILEVU's address and observed an individual that matches the appearance of ZILEVU at the residence.

16. Through my training and experience, I know that individuals who fraudulently obtain credit cards often try to avoid detection by dispersing charges amongst various types of retailers. The AMEX credit card statements listed multiple purchases made at various retailers. Security footages from some of the retailers showed an individual matching ZILEVU's description making purchases at the same time and location indicated on the AMEX credit card statements.

17. For instance, on or about January 3, 2017, the AMEX credit card was used to make a purchase totaling $217.27 at Lowe's of Dale City in Woodbridge, Virginia. Security footage from Lowe's of Dale City shows an individual matching ZILEVU's description inside the store on January 3, 2017, around 9:11 a.m. At 9:15 a.m., a person matching ZILEVU's description can be seen using a credit card at the cash register and exiting the store around 9:16 a.m. Surveillance video of the parking lot outside of Lowes on or about January 3, 2017, shows a tan Jeep Laredo heading toward the exit of the parking lot at 9:17 a.m. On or about February 28, 2017, agents conducted surveillance at ZILEVU's address, and observed a tan Jeep Laredo with a Vehicle Identification Number ("VIN") 1J4HR48N75C732. Agents ran the VIN number through a public database and learned that the vehicle is registered to ZILEVU and his mother.

18. Surveillance footage from Floor & Décor, located in Woodbridge, Virginia, shows a transaction on or about January 9, 2017, involving a person who matches the appearance of ZILEVU. On that same date, the AMEX credit card was used to make a purchase totaling $526.93 at Floor & Décor.

19. Surveillance footage from BJ Wholesale #0041 in Woodbridge, Virginia, shows a transaction on or about January 8, 2017, involving a person who matches the appearance of

ZILEVU. On that same date, the AMEX credit card was used to make a purchase totaling $405.67 at BJ Wholesale #0041.

20. On or about January 7, 2017, the AMEX credit card was used to make a purchase at Designer Shoe Warehouse ("DSW") in Woodbridge, Virginia. Surveillance footage from DSW on January 7, 2017, shows a person matching ZILEVU's description walking into DSW, approaching the counter, and purchasing merchandise.

21. Records obtained during the investigation also indicate that ZILEVU used the AMEX credit card to make a payment to himself on PayPal. On or about May 10, 2016, a request for $7,400 was sent from kzilevu@gmail.com to an email address similar to Victim A's true name, but does not belong to Victim A (hereinafter "Victim A's Fraudulent Email Account"). Google records obtained during the course of this investigation revealed that the email address kzilevu@gmail.com is registered to ZILEVU. During the September 2019 Interview, ZILEVU admitted that kzilevu@gmail.com is his email address. On or about April 11, 2017, ZILEVU received an email from service@paypal.com <service@paypal.com>. Even though the email was sent to kzilevu@gmail.com, the email was addressed to "MARCROTELE." At the September 2019 Interview, ZILEVU acknowledged owning and operating a business called MARCROTELE.

22. A note included with the May 10, 2016, request from kzilevu@gmail.com to Victim A's Fraudulent Email Account stated "MARCROTELE." Within minutes of the request being sent, Victim A's Fraudulent Email Account was accessed to transfer $7,400 to a PayPal account linked to kiddysmall@yahoo.com. ZILEVU admitted that the Yahoo email is his at the September 2019 Interview, and Yahoo records link this email to kzilevu@gmail.com and

ZILEVU's Google number. A review of the AMEX credit card statement showed a payment of $7, 400 to MARCROTELE on May 10, 2016.

23. There is also evidence showing that Victim A's Fraudulent Email Account was accessed on multiple occasions using a Verizon IP address registered to ZILEVU's address.

24. On or about May 13, 2016, the AMEX credit card was used to purchase two Delta plane tickets totaling $1,562.40. ZILEVU's address, ZILEVU's Google number, and email address kzilevu@gmail.com were provided to Delta airlines in connection with this purchase. On or about May 13, 2016, ZILEVU received an email to his kzilevu@gmail.com account from Delta Air Lines <DeltaAirLines@e.delta.com> confirming two round-trip ticket purchases totaling $1,562.40 for ZILEVU and another individual from Baltimore, Maryland, to Sacramento, California.

25. On or about November 13, 2016, ZILEVU received two emails sent to his kzilevu@gmail.com account from AmericanAirlines@aa.com addressed to Victim A. The first email confirmed the purchase of an American Airlines ticket for ZILEVU from Washington, DC, to Miami, Florida, on November 13, 2018. The second email was sent to confirm the purchase of a $21.79 seat upgrade for passenger ZILEVU on the November 13, 2016, flight. Both purchases were made using the AMEX credit card.

26. On or about November 14, 2016, ZILEVU received an email to his kzilevu@gmail.com account from HotelTonight <help@hoteltonight.com> confirming a hotel reservation for ZILEVU at the Riviera South Beach. This email advised that the AMEX credit card would be charged $100 for the room reservation. The AMEX credit card statement confirms the payment of $100.

27. From on or about October 11, 2016, to on or about January 13, 2017, ZILEVU paid for 37 Uber trips totaling $1,027.98 using the AMEX credit card. ZILEVU's Uber account showed that nine of the Uber trips taken during this time period either started or ended at ZILEVU's address.

28. A review of Amazon's records showed that the AMEX credit card was the primary payment method for an Amazon account in the name of ZILEVU's father. From on or about October 26, 2016, to on or about January 2, 2017, the AMEX credit card was used to make nine Amazon purchases totaling $1,200.00. The mailing address and telephone number on the account are ZILEVU's address and ZILEVU's Google number. A review of Microsoft records revealed that the email address for this account (skiddysmall@hotmail.com) is associated with ZILEVU's Google number. ZILEVU also confirmed that the Hotmail address is his at the September 2019 Interview.

29. VENMO records showed that on or about June 30, 2016, a VENMO account was opened in Victim A's name. The primary payment method for this account was the AMEX credit card. The email address used to register the VENMO account is similar to Victim A's true name and is the same email address used to create Victim A's Fraudulent Email Account. On or about July 7, 2016, an attempt to send a $500 payment for "Table @ park" to ZILEVU was made on the VENMO account opened in Victim A's name. On or about July 12, 2016, VENMO refunded the $500 for the July 7, 2016 transaction. On or about July 14, 2016, VENMO requested identification for the account opened in Victim A's name. On or about October 11, 2016, the account was cancelled and flagged as fraudulent.

30. A review of ZILEVU's Congressional Federal Credit Union account revealed that approximately ten electronic payments were made to the fraudulent AMEX account from

ZILEVU's Congressional Federal Credit Union account. It appears that ZILEVU was making the minimum monthly payment amount to AMEX, using his Congressional Federal Credit Union account, in order to keep the AMEX account open and active.

31. In or about June 2018, agents interviewed Victim A, who confirmed that the AMEX credit card had been taken out in his/her name, and that ZILEVU did not have permission or authority to use his/her information to apply for the AMEX credit card.

B. Victim B

32. On or about August 21, 2017, an electronic credit card application was submitted to U.S. Bank & Trust using PII of Victim B. The credit card account was approved and the credit card for this account was mailed to the address 5576 Roundtree Dr., Woodbridge, Virginia, 22193, which is the address of ZILEVU's parents ("Parents' address"). Law enforcement databases showed that this is ZILEVU's previous address and the current address of his parents. Additionally, agents observed ZILEVU at this residence on or about April 7 and December 29, 2017. Specifically, on or about April 7, 2019, agents observed ZILEVU drive from ZILEVU's address to ZILEVU's Parents' address.

33. An email address, which is not Victim B's email but is similar to Victim B's name, was listed on the U.S. Bank & Trust credit card application for Victim B. Google records associated with that email address revealed that the email address was accessed on multiple occasions by Verizon IP addresses assigned to ZILEVU's parents. The physical account address for the Verizon account of ZILEVU's parents was ZILEVU's address. The phone number for the account subscriber was a number ending in 0490 (hereinafter "ZILEVU's number"). T-Mobile records indicated that this number was assigned to ZILEVU. The Verizon account also

listed ZILEVU's Google number and the email address kzilevu@gmail.com as the contact information for the subscriber.

34. At least from on or around August 21, 2017, through at least on or around September 15, 2017, the U.S. Bank and Trust credit card statements revealed that a total of $10,273.39 in completed transactions and $2,651.62 in attempted transactions were made using the credit card issued in Victim B's name.

35. For instance, on or about September 8, 2017, the U.S. Bank and Trust credit card was used to make a purchase totaling $942.60 for a Delta Airlines plane ticket from Dulles Airport in Dulles, Virginia, to Montego Bay, Jamaica, for ZILEVU.

36. In or about August of 2019, agents interviewed Victim B, who confirmed that the fraudulent U.S. Bank & Trust credit card had been taken out in his/her name, and that ZILEVU did not have permission or authority to use his/her information to apply for the U.S. Bank & Trust Credit Card.

C. Victim C

37. On or about December 19, 2017, a credit card application was submitted to U.S. Bank & Trust using Victim C's PII. The primary address for the credit card listed Victim C's true address. The secondary address listed on this application is ZILEVU's address. When the credit card application was approved, the U.S. Bank & Trust credit card was mailed to ZILEVU's address.

38. The email address listed on the fraudulent U.S. Bank & Trust credit card application for Victim C is DoKay1933@gmail.com. A review of Google records associated with DoKay1933@gmail.com revealed that DoKay1933@gmail.com was accessed on multiple occasions by an internet protocol address assigned to Verizon subscriber ASEYE ZILEVU. The

physical account address for Verizon subscriber ASEYE ZILEVU is ZILEVU's address. The account lists ZILEVU's number, ZILEVU's Google number, and the email address kzilevu@gmail.com as the account holder's contact information.

39. The U.S. Bank and Trust credit card statements revealed that a total $9,641.69 in fraudulent charges were made using this credit card.

40. For instance, on or about December 30, 2017, the U.S. Bank and Trust credit card was used to purchase an Iceland Air ticket from Dulles Airport in Dulles, Virginia, to Reykjavik, Iceland, totaling $701.92. The passenger name listed on this plane ticket is ZILEVU.

41. A review of ZILEVU's official IRS email account, kwashie.s.zilevu@irs.gov, revealed that ZILEVU received an email from PayPal congratulating Victim C for setting up his/her account on or about February 2, 2018. This same email instructs Victim C to click a link in order to confirm that his/her email address, listed as kwashie.s.zilevu@irs.gov, is accurate. On or about February 3, 2018, ZILEVU received another email to his IRS email account from PayPal advising Victim C that he/she is officially a PayPal member.

42. In or about August of 2019, agents interviewed Victim C, who confirmed that the fraudulent U.S. Bank & Trust credit card had been taken out in his/her name, and that ZILEVU did not have permission or authority to use his/her information to apply for the U.S. Bank & Trust Credit Card.

D. Congressional Federal Credit Union

43. ZILEVU has a personal account with Congressional Federal Credit Union. On or about December 7, 2017, ZILEVU submitted a signed Affidavit of Loss to Congressional Federal Credit Union stating the following; "I was contacted by the credit union in regards to a potential deposit (check) that was made to my account which I do not have knowledge of. There

were series of charges made to my account of which I am also unaware of and disputing those charges." ZILEVU listed a total of 17 charges incurred between on or about November 29, 2017, to on or about December 5, 2017, that add up to $1,895.15. ZILEVU certified on the Affidavit of Loss that "I swear this affidavit is true and understand that making a false sworn statement is subject to federal and/or state statutes and may be punishable by fines and/or imprisonment." The affidavit was notarized in Fairfax County, Virginia.

44. A review of ZILEVU's email account and ZILEVU's own admissions during the September 2019 Interview suggests that ZILEVU falsely disputed at least some of the charges that he did, in fact, incur. For example, ZILEVU received booking confirmation numbers from Hotels.com for two reservations at the Plaza on the River in London, England. On or about November 30, 2017, ZILEVU received an email from Hotels.com. The subject of this email reads as follows; "Hotels.com booking confirmation 143502067830 - Plaza on the River – London." On or about November 30, 2017, ZILEVU also received an email from Visa Purchase Alerts. The subject of this email reads as follows; "Visa Purchase Alerts: 320.57 USD at HOTELS.COM143502067830 in HOTELS.COM on Card 9595." On or about December 1, 2017, ZILEVU received an email from Hotels.com. The subject of this email reads as follows; "Hotels.com booking confirmation 143527603137 - Plaza on the River – London." On or about December 1, 2017, ZILEVU received an email from Visa Purchase Alerts. The subject of this email reads as follows; "Visa Purchase Alerts: 216.93 USD at HOTELS.COM143527603137 in HOTELS.COM on Card 9595."

45. At the September 2019 Interview, ZILEVU admitted to going to London, England, on or about November 29, 2017, and returning to the United States on December 4, 2017. He also stated that he remembered staying at the Plaza on the River – London.

46. Law enforcement databases confirmed that on or about November 29, 2017, ZILEVU boarded an airplane at Dulles International Airport in Dulles, Virginia, destined for Heathrow International Airport, located in London, England, and that on or about December 4, 2017, ZILEVU boarded a return flight from Heathrow International Airport to Dulles International Airport.

CONCLUSION

47. Based on the information contained herein, I respectfully submit that there is probable cause to believe that from in or about January 2016 to in or about February 2018, in the Eastern District of Virginia, ZILEVU committed Access Device Fraud, in violation of Title 18, United States Code, Section 1029(a)(5).

Flannan Soden
Special Agent
Treasury Inspector General for Tax Administration

Subscribed and sworn to before me
on the 2nd day of October 2019.

/s/ JFA
John F. Anderson
United States Magistrate Judge

The Honorable John F. Anderson
United States Magistrate Judge
Alexandria, Virginia